Information Security Liaison Update

UAB Information Security
Agenda

• Policy & Rule Updates
• Email Data Loss Prevention
• DUO Security 2 factor authentication
• Sharing data with uab.box.com
• Security Awareness Training and Education Program
• Vulnerability Management & Pen Testing Program
• IPAM Update
• Security Exception Request Update
• Closing
Agenda

Policy, Rule & Guidelines Update
Policy, Rule & Guidelines Update

Policies
• Data Protection and Security Policy
• Data Access Policy
• Acceptable Use Policy

Rules
• Data Classification Rule
• Data Protection Rule
• Vulnerability Management Rule
• Security for Computing Device Rule
Policy, Rule & Guidelines Update

Guidelines

• Data custodian responsibilities
• Predefined data classifications
• Applying the Data Classification and Protection Rules
• Risk Level Assignment for UAB Restricted and Sensitive Data
• IT Guidelines for International Travel
• UAB Secure Application Development Guidelines
• Requirements for sharing Sensitive and Restricted/PHI via uab.box.com
• Encryption Guidelines
Upcoming Policy, Rule & Guidelines

Policies
• Access and Authentication Policy

Rules
• Password/Authentication Rule
• Access Management Rule
• Awareness/Training Rule
Agenda

Email Data Loss Prevention
Email Data Loss Prevention

• Enabling Microsoft’s Data Loss Prevention capabilities to identify, monitor, and automatically protect confidential information across our Email system.

  • Credit Card Numbers
  • Social Security Numbers
  • Protected Health Information (PHI)
Email Data Loss Prevention

You wouldn’t send sensitive information this way.

Post Card

Here is my info:
SSN: 438-018-0100
DOB: 06/31/91
VISA: 4469 3321 9876 3457

To anyone who
this card passes
along the way
NOT SECURE USA
Email Data Loss Prevention

“The content of this email appears to conflict with UAB Policy regarding unsecured transmission of Sensitive and Restricted data. If you do not resolve this conflict, this email may be blocked.”

• Process:
  • Content of email trips data loss prevention rules
  • Policy Tip (above) is displayed within the email client
  • Email is quarantined for SOC analysis
    • False-Positive – email is released for delivery
    • True–Positive – email is rejected (deleted), message sent back to user
Agenda

DUO Security 2 factor authentication
DUO Security 2 factor authentication

Two-factor authentication (2FA) leverages two separate methods of proving a user is who he or she claims to be.

UAB has selected Duo Security as its 2FA tool.

Benefits of 2FA

• Strengthen security around UAB institutional data
• Mitigate phishing vulnerabilities
• Duo users’ passwords no longer expire
DUO Security 2FA Project

May 2017 - Aug 2017 - completed -
• Integrate 2FA with CAS/Shibboleth
• Integrate 2FA with Box.com
• Pilot with select Duo users

Sept 2017 - Jan 2018 - in progress -
• Integrate 2FA with 150+ CAS/Shibboleth systems
• Expand to 400+ current Duo users
• Initiate opt in process for UAB community

Feb 2018 - Jan 2019
• Integrate 2FA with non-CAS and legacy systems
• Expand to high-risk individuals
• Continue promoting opt-in to UAB community

Feb 2019
• Revisit mandatory campus-wide 2FA participation
DUO Security 2 factor authentication

1. User enters BlazerID and password on application log in page
   • If individual is not a Duo user, continue with current process
   • If individual is a Duo user, automatically navigate to 2FA authentication page

2. Duo user chooses push or passcode

3. User completes 2FA
   • User can elect for Duo to remember their device for 30 days
http://www.uab.edu/it/home/2-factor
NIST’s New password rules (NIST SP 800-63-3: Digital Authentication Guidelines)

- **Favor the user.** To begin with, make your password policies *user friendly* and put the *burden on the verifier* when possible.
- **Check new passwords against a dictionary of known-bad choices.** Check for ChangeMe, Password1, abc123, ThisismyP@ssword!, etc.
- **Size does matter.** The longer the password, the longer it takes to crack.
- **No composition rules.** What this means is, no more rules that force you to use particular characters or combinations.
- **No more expiration without reason.** If we want users to comply and choose long, hard-to-guess passwords, we shouldn’t make them change those passwords unnecessarily.
New Password Expiration at UAB

• No more password expiration for DUO 2FA users.
  • The requirement for annual password change will be removed for DUO 2FA users.
  ** Please note that a password reset may still be required in the event of compromise **

• Password length will remain 15 characters
• Complexity requirements will be removed
Agenda

Sharing data with uab.box.com
Sharing data with uab.box.com

• The use of UAB Box must comply with all applicable laws, regulations and UAB policies.
  • Only UAB Box accounts are approved for storing UAB data that is classified as Sensitive or Restricted/PHI. Use of any other Box.com accounts (e.g. personal, starter, business, etc.) for storing Sensitive and/or Restricted/PHI UAB data is prohibited.
  • Likewise, the use of any similar Internet-based file sharing systems (such as Dropbox, GoogleDocs, etc.) for storing or sharing Sensitive or Restricted/PHI UAB data is prohibited, unless the system has been formally approved by the Office of the Vice President for Information Technology.
  • Storing cardholder data subject to the Payment Card Industry Data Security Standard (PCI DSS) in UAB Box is prohibited.
Handling HIPAA/PHI Restricted Data

• If you are processing ePHI with UAB Box or any other service, UAB HIPAA Policies require a completed and current risk assessment. The risk assessment form can be requested by sending an email to UAB Health System Information Security (HSIS) at riskassessments@uabmc.edu.
  • The request must include a description of the use case tied to sharing ePHI via UAB Box, along with specifics on the type of ePHI being shared and with whom it will be shared. HSIS will respond, provide a risk assessment template, and work with the requesting party in examining its needs and any associated risks.

• It is the responsibility of any user sharing PHI to ensure that who they are sharing with has been properly reviewed and has the proper contracts in place. Research projects are bound by data usage agreements specific to the research studies.

• Please be aware that the standard method is ShareFile for users with a uabmc.edu email.
Agenda

Security Awareness Training and Education
Security Awareness Training and Education

• Building the security awareness program this year
  • Website
  • Toolbox
    • Videos, Digital Signage, Gifs, Print, Social Media
  • Training available in LMS
  • National Cyber Security Awareness Month
    • Laptop Checkup
Security Awareness Toolkit
PhishMe Campaigns

• It is estimated that 90% of breaches are attributed to successful phishing campaigns
• Using PhishMe to empower our users to help strengthen defenses
  • Recognize and Report
Security Awareness Training and Education

- Plan for upcoming year
  - Targeted awareness and training
  - Targeted PhishMe campaigns
  - High Value Targets engagement
  - Participate in New Employee Orientation
  - Incident driven awareness and training
  - Quarterly events
  - National Cyber Security Awareness Month
Agenda

Vulnerability Management & Pen Testing
Vulnerability Management & Pen Testing

- The process used by University of Alabama at Birmingham Information Technology (UAB IT) in mitigating the risks from computer security vulnerabilities.

- Intended to represent a minimum baseline for managing vulnerabilities on UAB systems pursuant to the Data Protection and Security policy.
Vulnerability Management & Pen Testing

- Vulnerability Scan of all campus IPs minimum of monthly
- Ad-hoc
  - Coding changes
  - Network architecture changes
  - Upgrades
  - Incident Response
  - Firewall rule implementation
- InfoSec will work with information security liaisons, business units, and system owners to implement remediating actions

<table>
<thead>
<tr>
<th>Circumstances</th>
<th>VM</th>
<th>PT</th>
</tr>
</thead>
<tbody>
<tr>
<td>All campus IPs as normal production operation</td>
<td>Monthly</td>
<td>Annually</td>
</tr>
<tr>
<td>Any systems containing or processing sensitive/restricted data</td>
<td>Monthly</td>
<td>Annually</td>
</tr>
<tr>
<td>New system prior to become Internet facing</td>
<td>As Needed</td>
<td>As Needed</td>
</tr>
<tr>
<td>Major change with existing information system</td>
<td>As Needed</td>
<td>As Needed</td>
</tr>
<tr>
<td>Emerging threat due to newly discovered vulnerability</td>
<td>As Needed</td>
<td>N/A</td>
</tr>
<tr>
<td>Incident response and recovery</td>
<td>As Needed</td>
<td>As Needed</td>
</tr>
<tr>
<td>Required by applicable regulations or standards</td>
<td>As Prescribed</td>
<td>As Prescribed</td>
</tr>
</tbody>
</table>
Penetration Testing

- Internal Penetration Tester on staff
- Contract with third-party for annual external pen tester

- Timing, methodology, targets, and objectives of the penetration test are dependent upon the Rules of Engagement and scope as defined, drafted and agreed upon by the system owners and PT team

- Penetration tests are executed annually for critical systems or those hosting Restricted and/or Sensitive data as well as all production and Internet-facing systems
Agenda

IPAM Update
IPAM Update

- Systems entry and attestation
  - ~63% complete
  - Need your help in completing – dependency for other phases of project

- With attestation, we continue to ask that the ISLs use your best judgement in classification and record count. Ultimately we are attempting to answer the following questions, should a system be compromised:
  - How much data loss could occur?
  - How many people would need to be notified that their personal information was exposed?
  - What steps and notifications are we required to take by law, contract, or policy to address the exposure?

- We have included additional information on the ISL FAQ page
IPAM Update

IPAM - Ongoing
• IP address
• Inventory
• Classification
• Attestation
• Public
• Sensitive
• Restricted
• Additional
• system
• information

DNS – Jan 2018
• Replace
• existing DNS
• and Time
• servers
• New DNS
• views
• Internal
• External
• Department
• managed (via
• approval
• workflow)

DHCP – Jan 2018
• IP assignment
• centrally
• managed through IPAM
• DHCP
• Reserved
• assignments
• (no need for
• static IPs)
• DHCP pools
• available
• Custom DHCP
• options
• available

DRP – June 2018
• Dynamic
• Registration
• Portal
• User self
• service
• network
• registration
• User self
• service
• attestation
Security Exception Requests

Security Exception Request

University of Alabama at Birmingham (UAB) information security policies, standards, guidelines, and procedures establish controls that are used to protect institutional data and IT Resources. While any exception to a policy or standard can weaken protection for University IT Resources and data, occasionally exceptions will need to be made for legitimate University reasons. Information Security Liaisons and Departmental IT partners are responsible for ensuring enforcement of controls, and requesting exceptions to UAB information security policies and standard, and/or reviewing and re-validating the need for the exception with consideration of any appropriate data owner.

Exceptions can be requested for the following services:

- Firewall Rule Change - Request firewall rule changes
- Litigation Hold - Request litigation hold placed on an employee mailbox for content preservation
- Policy - Request exception to applications, networks and systems
- Third-Party Email Access - Request access to another employee's Exchange mailbox

Select Exception Form

-- None --

Order this Item
Delivery time 1 Day
Request Service
Add to Cart

Shopping Cart
Empty

UAB IT | IT Related Policies and Guidance
Disclaimer | UAB Web Pages Policy | © Copyright

UAB Information Security
Closing

- Continue to grow the ISL program
  - Communication is key

- Anything you need from us?
- Things we can do better?
Thanks for participating!

Knowledge that will change your world